

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

INTERNATIONAL AIRPORTS)	
CENTERS L.L.C., PIC IAC LLC and)	
IACEA LLC,)	
)	
Plaintiffs,)	No. 03 C 8104
)	
v.)	Wayne R. Andersen
)	District Judge
JACOB CITRIN,)	
)	
Defendant.)	

MEMORANDUM OPINION AND ORDER

This matter is before the court on defendant Jacob Citrin's motion to dismiss. Citrin has moved to dismiss Counts I, II, III, V and VI of the amended complaint filed by plaintiffs International Airport Center ("IAC"), PIC IAC, LLC and IACEA, LLC (collectively "plaintiffs"). Counts I, II, III and V allege claims that arise under state law, and Count VI alleges a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. For the following reasons, the motion to dismiss Count VI is granted, and plaintiffs' amended complaint is dismissed in its entirety.

BACKGROUND

In the amended complaint, plaintiffs allege both diversity and federal question jurisdiction. Citrin, however, asserts that this court does not have jurisdiction based on the diversity of the parties because defendant Citrin is a member of and owns a percentage interest in the plaintiff limited liability companies. Plaintiffs do not dispute a lack of diversity jurisdiction. Thus, subject matter jurisdiction in this court rests solely on Count VI, which is federal question

claim arising under the CFAA. The remaining claims are pendant state law claims. Therefore, we first will address whether plaintiffs have stated a claim under the CFAA.

For purposes of this motion, the following facts are taken as true. Plaintiff IAC is engaged in the business of owning, developing and operating structures designed to fulfill the warehouse, distribution and office needs of air freight companies and related users located in and around international airports. Citrin was an employee and managing director of IAC until October 30, 2003. During his employment, Citrin was responsible for identifying potential properties for acquisition by IAC and directing the acquisition process with respect to such properties. Plaintiffs assert that Citrin breached his contract and fiduciary obligations when he decided to leave his employment and compete with IAC. Plaintiffs allege that Citrin has fraudulently misappropriated IAC opportunities and assets along with confidential and proprietary work product.

Specifically, in relation to the allegations set forth in Count VI, plaintiffs assert that, prior to leaving his employment at IAC, Citrin deleted all of the data contained on the computer and snap backup server that IAC had provided him for his use as an IAC employee and managing director. In addition, IAC alleges that Citrin installed a software program on his computer and snap server that made it impossible for IAC to recover any of the deleted material. As a result of deleting this material and installing a program which prevented IAC from recovering any of the material, plaintiffs claim that Citrin has gained a competitive edge over IAC by having sole knowledge of the contents of the data he erased from his laptop computer and snap server. Based on these allegations, plaintiffs claim that Citrin has violated the CFAA, 18 U.S.C. § 1030(a)(5)(A).

DISCUSSION

To state a claim under the CFAA, a plaintiff must allege a knowing “transmission” of a “program, information, code, or command” to “protected computer” which causes damage. 18 U.S.C. § 1030(a)(5)(A) (2002); *Hayes v. Packard Bell Nec.*, 193 F. Supp. 2d 910, 912 (E.D. Tex. 2001). Plaintiffs allege that Citrin’s installation of a software program to delete the data and material stored on his individual laptop computer and backup snap server constitutes a violation of the CFAA. We disagree.

Even assuming as plaintiffs have alleged that Citrin “is guilty of gross spoilation in purging the data from the IAC computer and snap server” and that “by destroying the entire content of information contained on the computer and snap server, [Citrin] was clearly attempting to prevent IAC from recovering ... any evidence of his [alleged] improper conduct” (Amended Complaint, at ¶ 9), this court concludes that this conduct, as a matter of law, does not constitute a violation of the CFAA. The legislative history for the CFAA explains that the general purpose of the CFAA is to address the problem of computer crime, to protect computers and computer networks from access by hackers and to prevent the transmission of computer viruses or other harmful computer programs.

The scope of the CFAA has been expanded through various amendments since its enactment in 1984. Indeed, the Senate Report on the 1996 amendments recognizes that the CFAA is strengthened by the 1996 amendments and their attempt to “clos[e] gaps in the law to protect better the confidentiality, integrity and security of computer data and networks.” *See* S.Rep. No. 104-357, at 3 (1996). The report further provides that the CFAA:

facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology. As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the statute is up-to-date and provides law enforcement with the necessary framework to fight computer crime.

Id. at 5.

The question before us is whether the installation of a software program onto an individual laptop computer and backup snap server that was given to an employee for his individual use constitutes a “transmission” under the CFAA pursuant to section 1030(a)(5)(A). As a threshold matter, we note that there are very few cases which construe this section of the CFAA and the definition of “transmission”. *See* 18 U.S.C. § 1030(a)(5)(A); *North Texas Preventative Imaging v. Eisenberg*, 1996 WL 1359212 (C.D. Cal. Aug. 19, 1996); *Shaw v. Toshiba American Info. Sys., Inc.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999).

The *North Texas Preventative* court held that a “transmission” includes the creation of destructive microcode in California, the shipment of that destructive microcode via computer disk to Texas, and the down-loading of that destructive microcode from the disk onto the computer in Texas. *North Texas Preventative Imaging*, 1996 WL 1359212 , at * 7. The *Shaw* court held that a software developer of an allegedly defective microcode used in computer floppy-diskette controllers could be held liable under the CFAA for the third party sales of computers incorporating those controllers which contained the defective code. *Shaw*, 91 F. Supp. 2d at 936. Specifically, the *Shaw* court held that a “‘transmission’ includes the design, manufacture, creation, distribution, sale, transmission, and marketing of floppy-diskette controllers allegedly made faulty by defective microcode.” *Id.*

These courts in construing the term “transmission” have recognized that “transmission” includes the element of a shipment or delivery of a code or program, and plaintiffs argue that the allegations in the amended complaint also fall within the scope of the CFAA. Those allegations, in relevant part, state:

Citrin knowingly stripped by deliberate deletion of all the data from the IAC computer and snap server assigned to his use while a Managing Director of IAC. He then secretly imported a program into the computer and snap server that made it totally impossible for IAC to recover from the computer and/or snap server any of the deleted material, thus making it impossible for IAC to learn of either any of his activities or the information he obtained while a Managing Director that was contained in the computer and snap server....

(Amended Complaint at ¶ 9). Nowhere in the amended complaint do plaintiffs allege the shipment or delivery of a code or program as recognized by either the *North Texas Preventative* or *Shaw* courts.

Plaintiffs also rely on *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), as support for alleging a violation of the CFAA. In *Shurgard*, the plaintiff employer of former employees alleged to have misappropriated trade secrets stored on the employer’s computer sued the competitor who allegedly received the proprietary information through e-mails sent by the former employees while still employed by the plaintiff. Relying on subsections 1030(a)(2)(C), 1030(a)(4) and 1030(a)(5)(C) of the CFAA, the *Shurgard* court found that an employee’s misappropriation of trade secrets and the transmission of that information from the plaintiff to the defendant competitor via e-mail fell within the scope of the CFAA. These subsections impose liability on any person who “intentionally accesses a computer without authorization.”

Unlike the plaintiff in *Shurgard*, plaintiffs here assert a claim under subsection 1030(a)(5)(A) of the CFAA. Plaintiffs in this case do not seek relief under subsections 1030(a)(2)(C), 1030(a)(4) or 1030(a)(5)(C) because those subsections require that an individual “access” a computer “without authorization.” Plaintiffs do not assert that Citrin accessed a computer without authorization. In fact, plaintiffs admit that IAC provided a computer for Citrin to use during his employment at IAC, and the allegations in the amended complaint simply state that Citrin erased information from the computer and backup snap server before returning them to IAC.


All of these cases are distinguishable from the facts before us, and we find that the installation of a program which is designed simply to delete material only from that individual computer and snap server does not constitute a “transmission” as contemplated by the CFAA. We do not believe that Congress intended that the simple act of erasing files from an individual laptop computer and backup snap server would trigger liability under the CFAA, and we decline to expand the scope of the Act to include such conduct.

Plaintiffs’ amended complaint also includes allegations of misappropriation, conversion and alleged violations of the Illinois Trade Secret Act and the Illinois Computer Tampering Act. These allegations may state claims for relief although this court declines to decide those issues. This court, however, does find that the allegations in plaintiffs’ amended complaint do not fall within the scope of the CFAA. Based on the facts alleged in the amended complaint, plaintiffs fail, as a matter of law, to state a claim for a violation of the CFAA. Accordingly, we grant Citrin’s motion to dismiss Count VI. As the remaining claims in this case are pendent state law claims, we decline to exercise supplemental jurisdiction over those claims.

CONCLUSION

For the foregoing reasons, defendant's motion to dismiss Count VI is granted, and plaintiffs' amended complaint is dismissed in its entirety.

It is so ordered.



Wayne R. Andersen
United States District Judge

Dated: January 31, 2005